

# Grupo 20250417

## Integrantes

Nome	E-mail
<b>Ellen Heidi</b>	<a href="mailto:ellenheidi@gmail.com">ellenheidi@gmail.com</a>
<b>João Paulo</b>	<a href="mailto:joaopaulo_4@outlook.com">joaopaulo_4@outlook.com</a>
<b>Márcio</b>	<a href="mailto:marcio.mello@meta.com.br">marcio.mello@meta.com.br</a>
<b>Ricardo</b>	<a href="mailto:rsalomao1969@gmail.com">rsalomao1969@gmail.com</a>

link do projeto <https://github.com/rsalomao1969/ProjetoConciliacaoBancaria>

# **O Agente de Conciliação Inteligente: Um Plano Estratégico e Técnico para Automação Financeira de Alta Velocidade**

## **Seção 1: O Imperativo da Conciliação: Superando as Ineficiências Paralisantes dos Processos Manuais**

O contexto de negócios moderno exige velocidade, precisão e agilidade das funções financeiras. No entanto, um processo fundamental—a conciliação bancária—permanece, em muitas organizações, um bastião de ineficiência manual. Esta seção estabelece o contexto crítico ao dissecar as falhas profundas e dispendiosas dos fluxos de trabalho de conciliação tradicionais e manuais. A análise argumenta que este não é meramente um problema de eficiência, mas uma fonte significativa de risco financeiro, operacional e de conformidade que impacta diretamente o ciclo de fechamento financeiro e a tomada de decisões estratégicas.

### **1.1 A Anatomia da Falha da Conciliação Manual**

A conciliação manual é um processo inerentemente frágil, sobrecarregado por tarefas que são mal adequadas para a intervenção humana em escala. A pesquisa destaca que o processo é tedioso, repetitivo e ineficiente, especialmente ao lidar com grandes volumes de transações. Essa monotonia processual representa um uso inadequado das habilidades de profissionais de contabilidade altamente qualificados, que são relegados a tarefas mecânicas em vez de análise de alto valor.

Fundamentalmente, o processo é propenso a erros humanos. Isso inclui erros de entrada de dados, como a transposição de números (por exemplo, digitar \$5.243 em vez de \$5.423), entradas duplicadas que inflam artificialmente os saldos de caixa e distorcem as demonstrações financeiras, e classificações incorretas de transações. A dependência de planilhas para gerenciar esse processo agrava o risco. Ambientes que utilizam planilhas complexas com macros e fórmulas personalizadas, muitas vezes compreendidas por apenas alguns indivíduos, aumentam significativamente o perfil de risco da organização. Além disso, os processos manuais sofrem de uma gritante falta de padronização. Em organizações globais com várias entidades, cada departamento ou subsidiária pode operar com diferentes etapas de processo, formatos de planilha variados e conhecimento institucional isolado. Essa fragmentação cria caos na elaboração de relatórios finais e eleva o risco de conformidade. As planilhas, por sua natureza, carecem de controle de versão robusto e visibilidade em tempo real, forçando as equipes financeiras a trabalhar com números desatualizados e a gastar um tempo valioso reconciliando diferentes versões do mesmo arquivo.

### **1.2 As Consequências Estratégicas da Ineficiência**

As falhas processuais da conciliação manual se propagam para fora, gerando consequências estratégicas significativas que limitam a capacidade da função financeira de agregar valor.

- **Atraso no Fechamento Financeiro:** Os processos manuais são um dos principais gargalos que impedem o fechamento oportuno dos livros contábeis. Quanto maior o atraso, mais difícil se torna analisar discrepâncias, pois detalhes críticos são esquecidos, a equipe pode não se lembrar do contexto de uma transação específica e os logs do sistema de TI podem ser purgados, tornando a investigação forense quase impossível.
- **Crise de Escalabilidade:** À medida que os volumes de transações crescem—impulsionados por novos produtos, expansão de mercado ou adoção de métodos de pagamento adicionais—os processos manuais se tornam incontroláveis. Isso leva a custos crescentes, pois a única maneira de lidar com o aumento da carga de trabalho é um aumento linear no número de funcionários. O processo simplesmente não escala.
- **Oportunidades Estratégicas Perdidas:** O custo de oportunidade da ineficiência manual é imenso. Quando as equipes financeiras estão atoladas em tarefas manuais e de baixo valor, elas são incapazes de contribuir para análises estratégicas de maior valor. Em vez de analisar tendências de pagamento, otimizar estruturas de taxas ou modelar cenários de fluxo de caixa, a equipe fica presa no ciclo reativo de "fechar os livros". Eles se tornam guardiões de registros históricos em vez de parceiros estratégicos que impulsionam o negócio.

A dinâmica desses desafios cria um ciclo vicioso. A natureza tediosa e propensa a erros da conciliação manual leva ao esgotamento e à rotatividade de funcionários. Essa rotatividade resulta na perda de conhecimento institucional sobre nuances específicas de conciliação—como um determinado cliente formata seus extratos ou o que significam abreviações de memorando específicas. Com a perda desse conhecimento, novos funcionários são mais propensos a cometer erros e a criar seus próprios processos "paralelos" usando diferentes formatos de planilha, o que agrava a falta de padronização. Essa falta de padronização e o aumento da taxa de erros causam mais atrasos no fechamento financeiro e reduzem a confiabilidade dos relatórios financeiros. A baixa confiança nos dados, por sua vez, exige verificações e validações manuais ainda mais intensivas, intensificando a carga de trabalho e completando o ciclo de feedback negativo. Isso demonstra uma falha sistêmica, não apenas processual.

## Seção 2: Plano da Solução: O Agente de Conciliação Inteligente Alimentado por IA

Em resposta direta aos desafios paralisantes descritos na seção anterior, este plano apresenta uma solução transformadora: o Agente de Conciliação Inteligente. Esta seção introduz a solução em um nível elevado, enquadrando-a como uma resposta direta e poderosa aos problemas da conciliação manual. O propósito central da aplicação, o fluxo de trabalho do usuário e seu potencial transformador serão descritos.

### 2.1 Visão e Funcionalidade Central

O Agente de Conciliação Inteligente é uma aplicação web projetada para automatizar e aumentar o processo de conciliação bancária. Sua visão é transformar a conciliação de uma tarefa manual, propensa a erros e demorada, em um fluxo de trabalho inteligente, simplificado e orientado por dados.

A funcionalidade central do agente é ingerir documentos financeiros (por exemplo, extratos bancários, exportações do razão geral em formato CSV/XLSX), realizar a correspondência automatizada de transações e fornecer uma interface interativa para que os contadores gerenciem, investiguem e resolvam exceções com a assistência de um poderoso Modelo de Linguagem Grande (LLM). A aplicação visa automatizar a grande maioria das correspondências de transações, liberando os profissionais financeiros para se concentrarem nas discrepâncias que exigem julgamento humano e análise.

## 2.2 A Jornada do Usuário: Uma Mudança de Paradigma no Fluxo de Trabalho

O fluxo de trabalho do usuário com o Agente de Conciliação Inteligente representa uma mudança fundamental em relação aos processos tradicionais baseados em planilhas. A jornada é projetada para ser intuitiva, eficiente e colaborativa.

1. **Upload:** O usuário inicia o processo fazendo o upload seguro de um ou mais arquivos de dados financeiros (por exemplo, um extrato bancário e um extrato do razão correspondente) por meio de uma interface simples de arrastar e soltar.
2. **Correspondência Automatizada:** O backend do sistema processa instantaneamente os arquivos. Ele realiza uma primeira passagem de correspondência de alta confiança com base em critérios padrão, como valor, data e números de referência. Esta etapa resolve a maioria das transações "fáceis" em segundos.
3. **Tratamento de Exceções com IA:** Para as transações que não correspondem automaticamente, o sistema as apresenta em um painel claro e interativo. Aqui, o poder da IA é liberado. O usuário pode consultar a IA em linguagem natural (por exemplo, "Este memorando de transferência diz 'FAT1234-6', você pode combiná-lo com as faturas correspondentes?") para resolver correspondências complexas, ambíguas ou parciais.
4. **Visualização e Relatórios:** O usuário visualiza um painel em tempo real que resume o status da conciliação, incluindo taxas de correspondência automática, o envelhecimento dos itens em aberto e anomalias identificadas. Relatórios de conciliação finalizados podem ser gerados e exportados com um clique, fornecendo uma trilha de auditoria clara e documentação de suporte.

Esta solução proposta redefine fundamentalmente o papel do profissional de contabilidade. Ao automatizar entre 80% e 90% das tarefas de correspondência manuais e repetitivas, a aplicação eleva o usuário de um escriturário de entrada de dados a um investigador financeiro. O foco muda do trabalho entediante de marcar e conferir para o gerenciamento de exceções, a investigação de anomalias sinalizadas pela IA e a realização de análises de alto nível—tarefas que aproveitam seu julgamento profissional e expertise. Em vez de procurar uma agulha no palheiro, o sistema entrega as agulhas diretamente ao usuário para análise. Isso aborda diretamente os problemas de "escassez de pessoal" e "frustração" identificados na Seção 1, tornando o trabalho mais envolvente e estratégico.

## Seção 3: Mergulho na Arquitetura: Um Framework Moderno e Nativo de Python

Esta seção fornece a base técnica da solução, detalhando sua arquitetura e o fluxo de dados. A ênfase será em como a pilha de tecnologia escolhida cria um sistema coeso, eficiente e escalável, construído inteiramente dentro do ecossistema Python.

### 3.1 Visão Geral da Arquitetura Cliente-Servidor

A aplicação é construída sobre um modelo cliente-servidor moderno, que é crucial para implantá-la como uma aplicação web compartilhada e acessível por vários usuários.

- **Frontend (Cliente):** Um navegador da web executando uma interface construída com o Streamlit. O cliente é responsável por renderizar os componentes da interface do usuário (UI) e enviar as interações do usuário (uploads de arquivos, entradas de texto) para o servidor. É uma camada de apresentação leve.
- **Backend (Servidor):** Um processo Python iniciado pelo comando `streamlit run`. Este servidor hospeda a lógica da aplicação, é executado em uma única máquina (ou em um contêiner) e lida com toda a computação para todos os usuários simultâneos. Ele gerencia o processamento de dados com o Pandas e orquestra as chamadas de API para o LLM da Groq.

### 3.2 O Fluxo de Trabalho e de Dados Central

O fluxo de dados de ponta a ponta é projetado para ser lógico e eficiente, minimizando a latência e maximizando a automação.

1. **Ingestão de Arquivos:** O usuário interage com um widget `st.file_uploader` no frontend do Streamlit. Os arquivos enviados são transmitidos para o servidor backend e mantidos na memória para processamento.
2. **Análise e Normalização de Dados:** O backend usa o Pandas para ler os dados do arquivo em memória (por exemplo, `pd.read_csv`) e carregá-los em DataFrames. Esta etapa envolve etapas cruciais de limpeza e padronização para garantir que os dados de fontes diferentes possam ser comparados de forma confiável.
3. **Lógica de Correspondência Inicial:** O backend executa uma correspondência determinística baseada em regras dentro do Pandas para correspondências simples e um-para-um. Isso é computacionalmente barato e filtra as conciliações "fáceis", reduzindo a carga de trabalho para as etapas subsequentes.
4. **Análise Alimentada por LLM (para Exceções):** Para as transações restantes não correspondidas, o backend constrói um prompt cuidadosamente elaborado. Este prompt contém os dados relevantes (por exemplo, descrições de transações, valores, datas do DataFrame do Pandas) e é enviado para a API da Groq.
5. **Tratamento e Ação da Resposta:** A API da Groq retorna uma resposta estruturada (por exemplo, JSON) com correspondências sugeridas ou explicações. O backend analisa essa resposta e atualiza o estado da conciliação no DataFrame do Pandas.
6. **Atualização de Estado e Visualização:** O loop reativo do Streamlit detecta a mudança no estado da aplicação (ou seja, o DataFrame atualizado). A UI é automaticamente renderizada novamente para exibir o status de conciliação atualizado, incluindo tabelas interativas (`st.dataframe`) e gráficos gerados pelo Plotly.

A arquitetura inteira, do frontend à integração de IA do backend, é construída dentro de um ecossistema Python unificado. Essa abordagem de "pilha única" é uma vantagem estratégica significativa. Ela elimina a necessidade de equipes de desenvolvimento separadas para frontend (JavaScript/React) e backend, reduzindo a sobrecarga de comunicação e a complexidade do desenvolvimento. Isso permite que uma única equipe de cientistas de dados ou engenheiros financeiros com conhecimento de Python construa, itere e implante a aplicação.

em uma fração do tempo e do custo associados ao desenvolvimento de software empresarial tradicional, que envolve várias linguagens e frameworks. O Streamlit foi explicitamente projetado para permitir que desenvolvedores Python criem aplicações web "tudo em Python puro, sem necessidade de experiência em front-end". Essa escolha arquitetônica leva a uma prototipagem mais rápida, ciclos de iteração mais ágeis e um custo total de propriedade mais baixo, tornando-a uma abordagem altamente adequada para ferramentas financeiras internas ou novos produtos FinTech.

## **Seção 4: O Núcleo de Inteligência: Aproveitando a Groq para Conciliação de Alta Velocidade e Sensível ao Contexto**

Esta seção foca no "cérebro" da solução: o LLM da Groq. A análise argumenta que as características específicas da Groq—principalmente sua velocidade de inferência incomparável—não são apenas um "bônus", mas um facilitador crítico para operações financeiras que exigem resultados oportunos e uma experiência de usuário interativa.

### **4.1 A Necessidade de Velocidade na IA Financeira**

Processos financeiros como a conciliação são sensíveis ao tempo e impactam diretamente a velocidade do fechamento mensal ou trimestral. LLMs tradicionais podem introduzir latência, o que é inaceitável nesses fluxos de trabalho. A espera por uma resposta de IA interrompe o fluxo de trabalho do analista e degrada a usabilidade da ferramenta.

A Groq é projetada para inferência de latência ultrabaixa, fornecendo tempos de resposta que são múltiplos mais rápidos que os concorrentes. Essa velocidade é essencial para criar uma experiência de usuário interativa, onde as sugestões da IA parecem instantâneas, em vez de fazer o usuário esperar. Esse desempenho permite uma mudança da conciliação lenta em lote, realizada durante a noite, para um processo interativo e quase em tempo real, permitindo que os contadores fechem os livros mais rapidamente e com maior confiança.

### **4.2 Além da Correspondência Baseada em Regras: Automação Cognitiva com LLMs**

A automação tradicional depende de regras rígidas e predefinidas (por exemplo, "corresponder se o valor e o número da fatura forem idênticos"). Esses sistemas falham quando confrontados com dados não estruturados ou inconsistentes, que são comuns em transações financeiras. Os LLMs se destacam no tratamento de dados não estruturados e ambíguos, que são abundantes em descrições de transações financeiras. A solução proposta aproveitará a Groq para:

- **Analisar Texto Não Estruturado:** Interpretar campos de memorando complexos e abreviados. Por exemplo, a IA pode inferir que "FAT1234-6" se refere a três faturas separadas (1234, 1235 e 1236) e aplicar o pagamento de acordo.
- **Lidar com Variações de Dados:** Corresponder transações mesmo com variações nos nomes dos pagadores (apelidos, subsidiárias) ou inconsistências de formatação entre diferentes fontes de dados.

- **Inferência Contextual:** Utilizar padrões históricos e metadados para corresponder com confiança pagamentos que não possuem referências explícitas. Um exemplo seria quando o aviso de remessa chega em um e-mail separado; a IA pode analisar esse contexto externo para aplicar o pagamento corretamente.

### 4.3 Engenharia de Prompt Avançada para Precisão Financeira

Para garantir que o LLM forneça resultados financeiros precisos e confiáveis, serão empregadas técnicas sofisticadas de engenharia de prompt. Esta é a arte de elaborar instruções para guiar o raciocínio do modelo e restringir seu resultado.

- **Fornecimento de Contexto:** O prompt incluirá não apenas os dados da transação, mas também o esquema do banco de dados, definições de termos contábeis chave e exemplos de itens corretamente conciliados (prompting de poucas tentativas) para orientar o modelo.
- **Prompting de Cadeia de Pensamento:** O modelo será instruído a "pensar passo a passo", forçando-o a expor seu raciocínio para uma correspondência sugerida. Isso torna o processo mais transparente, auditável e menos propenso a "alucinações".
- **Saída Estruturada:** O prompt exigirá explicitamente que a saída seja em um formato JSON estruturado. Isso garante que ela possa ser analisada programaticamente pelo backend sem erros, evitando respostas "faladoras" ou inconsistentes que são difíceis de integrar em um fluxo de trabalho automatizado. Uma estrutura de prompt de exemplo seria:

```
Você é um assistente de contabilidade especialista. Dadas as duas séries de transações a seguir de um extrato bancário e de um razão geral, identifique as melhores correspondências possíveis. Para cada correspondência sugerida, forneça seu raciocínio. Retorne sua resposta APENAS em um formato JSON bruto com a seguinte estrutura:
```

A latência ultrabaixa da Groq faz mais do que apenas acelerar uma única etapa; ela muda fundamentalmente o modelo de interação do usuário. Em vez de um processo estático de "enviar e esperar", a velocidade da Groq permite um fluxo de trabalho dinâmico e conversacional. Um contador pode se envolver em um rápido bate-papo com a IA, refinando iterativamente suas consultas e explorando diferentes possibilidades de correspondência sem atrasos disruptivos. Um analista pode fazer uma pergunta inicial, ver o resultado instantaneamente e, em seguida, fazer imediatamente uma pergunta de acompanhamento com base nesse resultado (por exemplo, "Isso não está correto, agora tente combinar com os pagamentos de fornecedores da semana passada"). Esse fluxo iterativo e conversacional é muito mais poderoso para a resolução de problemas complexos do que uma consulta única e só é viabilizado pelo desempenho extremo do motor de inferência do LLM subjacente. Isso transforma a ferramenta de um simples automatizador em um verdadeiro parceiro colaborativo.

## Seção 5: A Experiência do Usuário: Um Hub de Conciliação Interativo com Streamlit e Plotly

Esta seção detalha o frontend da aplicação, enfatizando como o Streamlit e o Plotly se combinam para criar uma interface amigável, interativa e perspicaz que capacita os profissionais financeiros, em vez de sobrecarregá-los com complexidade.

### 5.1 Desenvolvimento Rápido de UI Nativa em Python com Streamlit

A proposta de valor central do Streamlit é sua simplicidade e velocidade de desenvolvimento. Ele permite transformar scripts de dados em aplicações web compartilháveis em minutos, usando Python puro, eliminando a necessidade de conhecimento em desenvolvimento web tradicional.

A solução aproveitará a rica biblioteca de widgets integrados do Streamlit para criar uma interface intuitiva :

- `st.file_uploader`: Para uma ingestão de arquivos fácil e segura, permitindo que os usuários arrastem e soltem seus extratos e livros-razão.
- `st.dataframe` e `st.data_editor`: Para exibir dados tabulares em um formato interativo, permitindo classificação, filtragem e até mesmo edições leves diretamente na interface.
- `st.sidebar` com `st.multiselect` e `st.date_input`: Para criar filtros poderosos e intuitivos que permitem aos usuários detalhar os dados por conta, período de tempo ou status.
- `st.text_input` ou `st.chat_input`: Para fornecer a interface de linguagem natural para consultar o agente de IA alimentado pela Groq.
- `st.columns` e `st.container`: Para organizar o layout em um painel limpo e profissional, apresentando as principais métricas e tabelas de dados de forma lógica.

### 5.2 Visualização Dinâmica de Dados com Plotly

Embora as tabelas de dados sejam essenciais, os painéis visuais fornecem insights rápidos sobre a saúde geral do processo de conciliação. O Plotly é a escolha ideal para criar gráficos interativos e de alta qualidade.

O painel contará com visualizações importantes:

- **Gráfico de Rosca:** Mostrando a proporção de transações que estão Conciliadas, Não Conciliadas e Conciliadas com assistência de IA.
- **Gráfico de Barras:** Exibindo o valor dos itens pendentes agrupados por idade (por exemplo, <30 dias, 30-60 dias, >60 dias) para destacar os riscos de envelhecimento.
- **Gráfico de Linha de Série Temporal:** Acompanhando a taxa de correspondência automática ao longo do tempo para medir a melhoria do processo.

Esses gráficos serão totalmente interativos, permitindo que os usuários passem o mouse para obter detalhes, apliquem zoom e panorâmica, proporcionando uma experiência muito mais rica do que relatórios estáticos e permitindo a exploração de dados diretamente no painel. A combinação da facilidade de uso do Streamlit com o poder das bibliotecas de IA/dados subjacentes democratiza a criação de ferramentas financeiras sofisticadas. Os departamentos financeiros não dependem mais exclusivamente de departamentos de TI centrais sobrecarregados ou de fornecedores terceirizados caros e inflexíveis. Uma equipe pequena e dedicada dentro do departamento financeiro—sejam "desenvolvedores cidadãos" ou uma

equipe de "FinOps"—pode construir e manter uma ferramenta personalizada que é perfeitamente adaptada aos seus fluxos de trabalho e formatos de dados específicos. Profissionais financeiros com habilidades em Python e análise de dados podem usar o Streamlit para construir suas próprias ferramentas, contornando os ciclos típicos de aquisição e desenvolvimento de software empresarial. Isso permite um novo modelo mais ágil de desenvolvimento de ferramentas internas, levando a soluções mais adequadas e a uma inovação mais rápida dentro da própria função financeira.

## Seção 6: Integridade e Processamento de Dados: O Papel Fundamental do Pandas

Esta seção detalhará o papel crítico da biblioteca Pandas como a espinha dorsal para toda a manipulação de dados, garantindo que os dados sejam limpos, estruturados e eficientemente preparados tanto para a correspondência baseada em regras quanto para a análise avançada de IA.

### 6.1 O Motor de Manipulação de Dados

O Pandas é o padrão de fato para análise de dados em Python, fornecendo estruturas de dados poderosas e eficientes como o DataFrame. Seu papel começa imediatamente após o upload do arquivo, onde ele lê vários formatos (CSV, Excel) em um DataFrame estruturado.

As principais etapas de pré-processamento realizadas com o Pandas incluem:

- **Limpeza de Dados:** Lidar com valores ausentes, corrigir tipos de dados (por exemplo, garantir que as datas sejam objetos datetime e os valores sejam numéricos) e remover entradas duplicadas para garantir a integridade dos dados.
- **Normalização:** Padronizar nomes de colunas e formatos de dados (por exemplo, formatos de data, símbolos de moeda) de fontes díspares para criar um esquema unificado para comparação. Esta é uma etapa crítica para o sucesso da correspondência.
- **Engenharia de Recursos:** Criar novas colunas que podem auxiliar na correspondência, como extrair números de fatura potenciais de campos de memorando usando expressões regulares, ou calcular a diferença absoluta entre valores para identificar correspondências próximas.

### 6.2 Melhores Práticas para a Interface com o LLM

Enviar DataFrames inteiros e grandes para um LLM é ineficiente, caro e pode levar a um desempenho ruim devido às limitações da janela de contexto e ao problema de "agulha no palheiro", onde a informação relevante se perde em um mar de dados irrelevantes.

A estratégia adotada será usar o Pandas para pré-processamento e filtragem, e então passar apenas o contexto mínimo necessário para a API da Groq. O fluxo de trabalho é o seguinte:

1. Usar o Pandas para realizar todas as correspondências determinísticas possíveis primeiro.
2. Isolar as transações restantes, difíceis de corresponder, em um DataFrame de "exceções" menor.

3. Para cada exceção, extrair apenas a(s) linha(s) relevante(s) e um pequeno número de transações potencialmente relacionadas (por exemplo, transações com valores semelhantes no mesmo período).
4. Serializar este pequeno subconjunto de dados em um formato conciso (como CSV ou uma string formatada) para ser incluído no prompt, juntamente com os metadados do DataFrame (nomes das colunas, tipos de dados). Isso minimiza o uso de tokens e foca a atenção do LLM no problema específico.

Nesta arquitetura, o Pandas não é apenas um contêiner de dados; ele atua como um "filtro cognitivo" crucial que otimiza o desempenho e a relação custo-benefício do LLM. As chamadas de API do LLM são precificadas por token, e o desempenho se degrada com contextos excessivamente grandes. Um arquivo de conciliação típico pode ter milhares de transações, mas a maioria são correspondências simples. Usar o Pandas para realizar essas correspondências simples é computacionalmente muito barato e rápido. Esta primeira passagem pode resolver 80% das transações, deixando apenas 20% como exceções. Em vez de enviar 100% dos dados para o LLM, a solução só precisa enviar os 20% que requerem raciocínio avançado. Isso reduz drasticamente o número e o tamanho das chamadas de API, cortando diretamente os custos operacionais e melhorando os tempos de resposta. Portanto, a divisão inteligente do trabalho entre o Pandas e o LLM é uma otimização arquitetônica fundamental.

## Seção 7: Medindo o Sucesso: Métricas de Desempenho e Retorno sobre o Investimento (ROI) Esperado

Esta seção traduzirá as capacidades técnicas da solução em um caso de negócios financeiro e operacional convincente. Serão definidas métricas claras para o sucesso e projetado um forte ROI com base em dados da indústria e estudos de caso.

### 7.1 Indicadores Chave de Desempenho (KPIs) para a Excelência na Conciliação

Um conjunto de KPIs mensuráveis será definido para acompanhar o desempenho da solução e do próprio processo de conciliação, com base nas melhores práticas do setor.

- **Taxa de Correspondência Automática:** A porcentagem de transações correspondidas automaticamente sem intervenção humana. (Meta de referência: >90%).
- **Taxa de Precisão da Conciliação:** Porcentagem de conciliações concluídas com zero erros. (Meta de referência: >99%).
- **Tempo de Ciclo da Conciliação:** O tempo médio desde o início do processo até sua conclusão. (Meta: Reduzir em >50%).
- **Idade dos Itens Pendentes:** Uma análise dos itens não conciliados por idade, com o objetivo de eliminar itens com mais de 30 dias.
- **Custo por Conciliação:** O custo total (incluindo tempo da equipe e custos do sistema) para concluir o processo.

## 7.2 Projetando o Retorno sobre o Investimento (ROI)

Com base em estudos empíricos sobre IA na automação de processos financeiros, um modelo de ROI robusto será construído.

- **Economia de Custos Diretos (Redução de Mão de Obra):** Pesquisas indicam que a automação pode reduzir o tempo de conciliação manual em até 80-90%. Isso será modelado calculando as horas economizadas para a equipe financeira, que podem ser realocadas para iniciativas estratégicas. Estudos mostram uma economia média anual de mão de obra de \$2.3 milhões em automação financeira mais ampla.
- **Benefícios Financeiros Indiretos:**
  - **Redução da Taxa de Erros:** Processos aprimorados por IA podem reduzir o retrabalho em até 85% , evitando os custos associados à correção de demonstrações financeiras e à tomada de decisões ruins com base em dados falhos.
  - **Melhoria na Gestão do Fluxo de Caixa:** Uma conciliação mais rápida fornece uma visão mais clara e oportuna das posições de caixa, permitindo melhores decisões de investimento e empréstimo.
  - **Redução dos Custos de Auditoria:** Processos de conciliação limpos, auditáveis e bem documentados podem reduzir os honorários de auditoria externa em até 35%.
- **Projeção Geral do ROI:** Com base nesses fatores, estudos mostram um ROI típico para projetos de automação de conciliação na faixa de 80-150% no primeiro ano. O ROI deste sistema se estende para além do departamento financeiro. Um processo de conciliação mais rápido e preciso cria uma única fonte de verdade para a posição de caixa da empresa. Esses dados de alta qualidade e em tempo real se tornam um ativo fundamental que melhora a qualidade da tomada de decisões em toda a organização—desde a tesouraria e o Planejamento e Análise Financeira (FP&A) até as vendas e operações. O investimento inicial na automação da conciliação, portanto, tem um efeito multiplicador na inteligência de negócios e na agilidade geral da empresa. Quando os dados fundamentais são mais oportunos e precisos, a qualidade e a confiabilidade de todas as análises e modelos estratégicos subsequentes são inerentemente aprimoradas. O investimento não otimiza apenas um processo; ele aprimora a qualidade de toda a cadeia de suprimentos de dados financeiros.

## Seção 8: Cenário Competitivo e Posicionamento Estratégico

Esta seção situará a solução proposta no mercado existente de software de conciliação financeira, destacando sua proposta de valor única e suas vantagens competitivas.

### 8.1 O Cenário Existente: Suítes de Fechamento Financeiro Empresarial

O mercado é atualmente dominado por grandes players estabelecidos que oferecem suítes abrangentes de fechamento financeiro. Os principais concorrentes incluem:

- **BlackLine:** Líder de mercado conhecido por sua plataforma em nuvem para gerenciamento de operações financeiras, com foco na modernização da contabilidade e na garantia de visibilidade.
- **Trintech (Cadency, Adra):** Fornece soluções baseadas em nuvem para correspondência de transações de alto volume, conciliação de balanço e gerenciamento de fechamento para grandes empresas e empresas de médio porte.
- **HighRadius:** Foca em conciliação e gerenciamento de tesouraria em escala empresarial, alimentados por IA.
- **Outros Players:** Sage Intacct, Oracle NetSuite, FloQast, que frequentemente integram a conciliação em plataformas maiores de ERP ou contabilidade.

## 8.2 Nossos Diferenciais: Agilidade, Customização e Velocidade

A solução proposta não se destina a ser um substituto direto, recurso por recurso, para essas plataformas monolíticas. Em vez disso, ela se posiciona como uma ferramenta mais ágil, moderna e focada, que oferece vantagens distintas.

**Tabela 8.1: Análise Comparativa de Recursos**

Esta tabela fornece uma comparação clara e rápida da solução proposta em relação a três concorrentes principais, permitindo que os stakeholders entendam rapidamente onde a solução se destaca e como ela se difere dos sistemas empresariais estabelecidos.

Recurso	Agente de Conciliação Inteligente (Nossa Solução)	BlackLine	HighRadius	Sage Intacct
<b>Tecnologia de IA Central</b>	LLM de alta velocidade (Groq) para automação cognitiva e análise de dados não estruturados.	Principalmente baseado em regras com ML para sugestões.	IA/ML para correspondência de transações e detecção de anomalias.	Correspondência automatizada dentro de um contexto de ERP.
<b>Modelo de Implantação</b>	Altamente flexível (onpremise, nuvem privada) via implantação do Streamlit.	SaaS (Software como Serviço).	SaaS.	SaaS (parte do ERP).

<b>Customização</b>	Extremamente alta. Construído em uma pilha de código aberto, permitindo profunda customização da lógica e da UI.	Moderada. Configuração dentro dos limites da plataforma.	Moderada a Alta. Configurável, mas dentro de um ecossistema proprietário.	Baixa a Moderada. Limitada às capacidades do módulo ERP.
<b>Velocidade de Desenvolvimento</b>	Muito rápida. Prototipagem e iteração rápidas com o Streamlit.	N/A (desenvolvimento orientado pelo fornecedor).	N/A.	N/A.
<b>Usuário-Alvo</b>	Equipes financeiras com habilidades em Python ("FinOps"), FinTechs buscando um componente central.	Departamentos de contabilidade de grandes empresas.	Grandes empresas com altos volumes de transações.	Pequenas a grandes empresas que usam o ERP Sage.
<b>Recurso</b>	<b>Agente de Conciliação Inteligente (Nossa Solução)</b>	<b>BlackLine</b>	<b>HighRadius</b>	<b>Sage Intacct</b>
<b>Integração</b>	Design API-first, facilmente integrável com qualquer sistema via Python.	Conectores pré-construídos para os principais ERPs.	Conectores pré-construídos.	Integração profunda dentro do ecossistema Sage.

A solução proposta representa uma tendência mais ampla no software empresarial: o "desmembramento" de grandes suítes monolíticas em ferramentas especializadas e de melhor qualidade. Enquanto plataformas como a BlackLine oferecem uma solução completa, o agente proposto fornece um componente de alto desempenho e hiper focado para conciliação, que pode ser integrado à pilha financeira personalizada existente de uma empresa. Essa abordagem permite que uma empresa adote uma estratégia de "empresa componível", onde seleciona a melhor ferramenta para cada trabalho específico e as integra, em vez de ficar presa ao roteiro e às escolhas tecnológicas de um único fornecedor. Isso posiciona a solução não como uma versão inferior de uma suíte empresarial, mas como uma escolha estratégica para empresas que valorizam flexibilidade, desempenho e controle sobre sua pilha de tecnologia.

## Seção 9: Roteiro de Implementação e Gestão da Mudança

Esta seção fornecerá um plano prático e acionável para implantar a solução e garantir sua adoção bem-sucedida dentro da organização financeira, reconhecendo que a mudança tecnológica é também uma mudança humana.

### 9.1 Estratégia de Implementação em Fases

1. **Fase 1: Programa Piloto (Semanas 1-4):** Começar pequeno com um caso de uso único e bem definido (por exemplo, conciliar uma conta bancária principal para uma unidade de negócios). Isso permite o desenvolvimento rápido, testes e coleta de feedback dos stakeholders com o mínimo de interrupção.
2. **Fase 2: Expansão e Integração (Semanas 5-10):** Com base no feedback do piloto, expandir a solução para incluir mais contas e unidades de negócios. Desenvolver as integrações necessárias com sistemas upstream/downstream (por exemplo, feeds de dados automatizados do ERP).
3. **Fase 3: Lançamento Completo e Otimização (Semanas 11+):** Implantar a solução em toda a organização. Estabelecer um modelo de governança e iniciar o monitoramento contínuo dos KPIs para identificar novas oportunidades de otimização.

### 9.2 O Elemento Humano: Um Plano Proativo de Gestão da Mudança

A adoção de IA frequentemente enfrenta resistência devido ao medo da perda de empregos ou ao desafio de aprender novas habilidades. Um plano estruturado de gestão da mudança é essencial para o sucesso.

- **Comunicação e Visão:** A liderança deve comunicar de forma clara e consistente a visão para o agente de IA—não como um substituto para os contadores, mas como uma ferramenta de aumento que elimina o trabalho tedioso e permite uma análise estratégica de maior valor.
- **Treinamento e Qualificação:** Fornecer treinamento abrangente sobre como usar a nova ferramenta de forma eficaz. Isso inclui não apenas "como clicar nos botões", mas também "como pensar como um investigador financeiro" com um parceiro de IA. Isso constrói confiança e demonstra um compromisso com o crescimento dos funcionários.
- **Identificar Campeões:** Cultivar os primeiros adeptos e entusiastas dentro da equipe financeira para atuarem como campeões, fornecendo apoio aos colegas e demonstrando os benefícios do novo fluxo de trabalho.
- **Ciclos de Feedback:** Estabelecer canais claros para que os usuários forneçam feedback durante o piloto e além, tornando-os participantes ativos na evolução da ferramenta. A implementação desta ferramenta é mais do que um projeto de melhoria de processos; é um catalisador para a transformação estratégica do departamento financeiro. À medida que a automação lida com tarefas transacionais, as habilidades exigidas dos profissionais financeiros mudarão da entrada e manipulação de dados para a análise de dados, interpretação estratégica e comunicação interfuncional. O plano de gestão da mudança, portanto, deve ser uma estratégia de desenvolvimento de talentos a longo prazo, não apenas um plano de lançamento de software a curto prazo. O sucesso

do projeto não é apenas uma aplicação totalmente funcional, mas uma equipe financeira que opera em um nível estratégico mais elevado.

## Seção 10: Estrutura de Segurança e Governança para Dados Financeiros

Esta seção final aborda a importância primordial da segurança e da governança de dados, detalhando as medidas que serão implementadas para proteger informações financeiras sensíveis e garantir a conformidade regulatória.

### 10.1 Princípios Fundamentais de Segurança

Uma abordagem de "segurança por design" será adotada, integrando considerações de segurança em todas as etapas do ciclo de vida do desenvolvimento.

- **Minimização de Dados:** O princípio de processar apenas os dados absolutamente necessários será aplicado. Ao interagir com o LLM, apenas os dados mínimos necessários para resolver uma exceção específica serão enviados, não arquivos inteiros.
- **Sanitização de Entradas e Filtragem de Saídas:** Todas as entradas do usuário (prompts) serão sanitizadas para prevenir ataques de injeção de prompt. Todas as saídas do LLM serão validadas e filtradas para garantir que não contenham informações sensíveis ou conteúdo malicioso antes de serem exibidas ou armazenadas.

### 10.2 Controle de Acesso e Manuseio de Dados

- **Controle de Acesso Baseado em Funções (RBAC):** A aplicação implementará um RBAC rigoroso, garantindo que os usuários possam acessar e conciliar apenas as contas para as quais estão autorizados.
- **Armazenamento e Trânsito Seguros de Dados:** Todos os dados sensíveis, seja em repouso em um banco de dados ou em trânsito entre o servidor e a API da Groq, serão criptografados usando protocolos padrão da indústria como AES-256 e TLS.
- **Uso Seguro de API:** As chaves de API para o serviço da Groq serão armazenadas de forma segura (por exemplo, usando um sistema de gerenciamento de segredos) e a comunicação será limitada por taxa para prevenir ataques de negação de serviço.

### 10.3 Auditabilidade e Conformidade

Uma trilha de auditoria abrangente será mantida, registrando cada ação realizada no sistema—desde uploads de arquivos até substituições manuais e correspondências sugeridas pela IA. Isso proporciona total transparência e é crítico para controles internos e auditorias externas. O sistema será projetado para ajudar a impor a conformidade com as regulamentações financeiras, fornecendo um processo de conciliação padronizado, documentado e verificável.

No contexto dos LLMs, a engenharia de prompt não é apenas uma ferramenta para melhorar a precisão; é um controle de segurança crítico. Um dos principais riscos dos LLMs é a injeção de prompt, onde a entrada de um usuário engana o modelo para que ele ignore suas instruções originais. Outro risco é o vazamento de dados, onde o modelo revela inadvertidamente

informações sensíveis de seu contexto. Ao usar prompts altamente estruturados que definem estritamente os formatos de entrada e saída esperados (por exemplo, exigindo saída JSON), a superfície de ataque para injeção de prompt e vazamento de dados é significativamente reduzida. Um prompt bem projetado atua como um "contrato" com o LLM, restringindo seu comportamento e tornando menos provável que ele se desvie de maneiras inesperadas ou inseguras. Esse formato restrito torna muito mais difícil para um invasor injetar instruções que levariam à execução de código arbitrário ou a uma resposta narrativa contendo dados vazados. O modelo é forçado a responder dentro da estrutura rígida do esquema JSON. Portanto, o ato de projetar o prompt é uma parte central da arquitetura de segurança da aplicação, servindo como um firewall semântico.

## **Seção 11: Conclusão: Uma Nova Era de Operações Financeiras**

Esta seção final resumirá os principais argumentos e reiterará o potencial transformador do Agente de Conciliação Inteligente.

### **11.1 Resumo da Proposta**

Foi apresentada uma solução que aborda diretamente as ineficiências crônicas e os riscos da conciliação bancária manual, aproveitando uma pilha de tecnologia moderna, ágil e poderosa. A combinação do desenvolvimento rápido do Streamlit, do robusto manuseio de dados do Pandas, das visualizações perspicazes do Plotly e da inferência de IA de alta velocidade da Groq cria uma proposta de valor única e convincente.

### **11.2 O Imperativo Estratégico**

A adoção desta solução não é meramente uma atualização operacional; é um investimento estratégico no futuro da função financeira. Ela promete reduzir custos, acelerar o fechamento financeiro, aprimorar a conformidade e—o mais importante—liberar o talento humano para se concentrar na análise estratégica que impulsiona o valor do negócio. O Agente de Conciliação Inteligente representa o futuro das operações financeiras: inteligente, ágil e orientado por dados.

### **Referências citadas**

1. Challenges of Manual Reconciliation Processes for Electronic Payment Acceptance, <https://reconhub.cloud/en/insights/continuous-accounting/challenges-of-manual-reconciliation-processes-for-electronic-payment-acceptance> 2. The 5 Most Common Bank Reconciliation Errors – And How to Avoid Them, <https://www.cashmanagement.org/bank-reconciliation/the-5-most-common-bank-reconciliation-errors-and-how-to-avoid-them/> 3. Why Manual Reconciliation Fails Accounting Teams - Teampay, <https://www.teampay.co/blog/problems-with-manual-reconciliation> 4. 4 Manual Reconciliation Problems You Need to Solve - Trintech, <https://www.trintech.com/blog/manualreconciliation-problems-to-solve/> 5. Learn About the Disadvantages of Manual Bank Reconciliation - Paystand, <https://www.paystand.com/blog/disadvantages-of-manual-bankreconciliation> 6. 7 Use Cases Of

AI-Based Account Reconciliation Software - HighRadius, <https://www.highradius.com/resources/Blog/account-reconciliation-software-use-cases/> 7. 3 Use Cases of Account Reconciliation Automation - Trintech, <https://www.trintech.com/blog/reconciliation-account-automation-use-cases/> 8. Understanding Streamlit's client-server architecture, <https://docs.streamlit.io/develop/concepts/architecture/architecture> 9. Streamlit Upload File: Mastering File Upload and Display with Python - Kanaries Docs, <https://docs.kanaries.net/topics/Streamlit/streamlit-upload-file> 10. st.file\_uploader - Streamlit Docs, [https://docs.streamlit.io/develop/api-reference/widgets/st.file\\_uploader](https://docs.streamlit.io/develop/api-reference/widgets/st.file_uploader) 11. [Python] Streamlit for Data Mining Visualization | by Amiruddin Saddam - Medium, <https://medium.com/learning-about-data-mining/streamlit-for-data-mining-visualization-4a3efec1455b> 12. 8 AI reconciliation use cases and examples - Ledge, <https://www.ledge.co/content/aireconciliation> 13. Optimizing Financial Market Data with pandas: Analysis and Transformation | by Merlyn Shelley @PacktPub | Packt Hub | Medium, <https://medium.com/packt-hub/optimizing-financial-market-data-with-pandas-analysis-and-transformation-e330f1b0b37a> 14. Introduction to Tool Use - GroqDocs, <https://console.groq.com/docs/tool-use> 15. Process Pandas DataFrames with a Large Language Model | Towards Data Science, <https://towardsdatascience.com/process-pandas-dataframes-with-a-large-language-model-8362468aca47/> 16. Getting Structured JSON Responses from LLMs: A Simple Solution - Python in Plain English, <https://python.plainenglish.io/getting-structured-json-responses-fromllms-a-simple-solution-f819fc389ebc> 17. How to Combine Streamlit, Pandas, and Plotly for Interactive Data Apps - KDnuggets, <https://www.kdnuggets.com/how-to-combine-streamlit-pandas-and-plotly-forinteractive-data-apps> 18. Building a dashboard in Python using Streamlit, <https://blog.streamlit.io/crafting-a-dashboard-app-in-python-using-streamlit/> 19. Streamlit • A faster way to build and share data apps, <https://streamlit.io/> 20. How We Built an AI-powered Capital Markets Research Platform with Streamlit: A Case Study - Show the Community!, <https://discuss.streamlit.io/t/how-we-built-an-ai-powered-capital-markets-research-platform-with-streamlit-a-case-study/78746> 21. Enabling LLMOps with Fast AI Inference - Groq, <https://groq.com/customer-stories/groq-customer-use-case-orq> 22. AI-powered Financial Insights | Groq is fast, low cost inference., <https://groq.com/customer-stories/groq-customeruse-case-fintool> 23. A Survey of Large Language Models for Financial Applications: Progress, Prospects and Challenges - arXiv, <https://arxiv.org/html/2406.11903v1> 24. Prompt Engineering: The Ultimate AI Skill for Investment Operations - Empaxis, <https://www.empaxis.com/blog/prompt-engineering> 25. Prompt Engineering for Finance 101 | Deloitte US, <https://www.deloitte.com/us/en/services/consulting/articles/prompt-engineering-for-finance.html> 26. Generative AI based virtual assistant for reconciliation research - Amazon Science, <https://www.amazon.science/publications/generative-ai-based-virtual-assistant-for-reconciliation-research> 27. Building a Streamlit AI summarizer over JSON APIs | ft. Pydantic - YouTube, <https://www.youtube.com/watch?v=RjpFMiv-1JA> 28. App Gallery - Streamlit, <https://streamlit.io/gallery> 29. Creating a Financial Dashboard Using Python and Streamlit | Towards Data Science, <https://towardsdatascience.com/creating-a-financial-dashboard-usingpython-and-streamlit-ccc6c026676/> 30. Building an Interactive Financial Dashboard with Streamlit and Plotly: A StepbyStep Tutorial | by Karthikeya Reddy | Medium,

<https://medium.com/@reddykarthikeya1/building-an-interactive-financial-dashboard-with-streamlit-and-plotly-a-step-by-step-tutorial-4b9973b62be5> 31. Chat with pandas DataFrames using LLMs - Streamlit Blog, <https://blog.streamlit.io/chat-with-pandas-dataframes-using-llms/> 32. Plotly: Data Apps for Production, <https://plotly.com/> 33. Financial charts in Python - Plotly, <https://plotly.com/python/financial-charts/> 34. Plotly Python Graphing Library, <https://plotly.com/python/> 35. Financial Analytics Using Python and AI Tools - Dan Gode, <https://www.dangode.com/financialanalytics/> 36. Python and Statistics for Financial Analysis | Coursera, <https://www.coursera.org/learn/python-statistics-financial-analysis> 37. 3 examples of using pandas for financial market data analysis - PyQuant News, <https://www.pyquantnews.com/the-pyquant-newsletter/3-examples-pandas-financial-market-data-analysis> 38. 10 minutes to pandas — pandas 2.3.3 documentation, [https://pandas.pydata.org/docs/user\\_guide/10min.html](https://pandas.pydata.org/docs/user_guide/10min.html) 39. Best way to pass pd.Dataframes in context : r/LangChain - Reddit, [https://www.reddit.com/r/LangChain/comments/1jsox0p/best\\_way\\_to\\_pass\\_pddataframes\\_in\\_context/](https://www.reddit.com/r/LangChain/comments/1jsox0p/best_way_to_pass_pddataframes_in_context/) 40. LLMs + Pandas: How I Use Generative AI to Generate Pandas DataFrame Summaries, <https://towardsdatascience.com/llms-pandas-how-i-use-generative-ai-to-generate-pandas-dataframe-summaries-2/> 41. Key Metrics for Measuring Accounts Reconciliation Performance, <https://www.goconstant.com/blog/key-metrics-for-measuring-accounts-reconciliation-performance> 42. Account Reconciliation Rate - RCM Metrics - MD Clarity, <https://www.mdclarity.com/rcmmetrics/account-reconciliation-rate> 43. (PDF) The return on investment (ROI) of intelligent automation: Assessing value creation via AI-enhanced financial process transformation - ResearchGate, [https://www.researchgate.net/publication/394436747\\_The\\_return\\_on\\_investment\\_ROI\\_of\\_intelligent\\_automation\\_Assessing\\_value\\_creation\\_via\\_AI-enhanced\\_financial\\_process\\_transformation](https://www.researchgate.net/publication/394436747_The_return_on_investment_ROI_of_intelligent_automation_Assessing_value_creation_via_AI-enhanced_financial_process_transformation) 44. How Reconciliation Automation Can Save Your Finance Team Time and Money - Kosh.ai, <https://www.kosh.ai/blog/how-reconciliation-automation-can-save-your-finance-team-time-and-money> 45. Finance AI: Transforming Financial Operations & Decision-Making - Coupa, <https://www.coupa.com/blog/finance-ai-how-ai-used-finance-and-how-can-it-improve-organizational/> 46. How AI Is Changing Corporate Finance in 2025 - Workday, <https://www.workday.com/en-us/perspectives/finance/2025/03/how-ai-changing-corporate-finance-2025.html> 47. 12 Best Reconciliation Tools: Ultimate Guide 2026 - Solvexia, <https://www.solvexia.com/blog/5-best-reconciliation-tools-complete-guide> 48. Best Financial Reconciliation Solutions Reviews 2025 | Gartner Peer Insights, <https://www.gartner.com/reviews/market/financial-reconciliation-solutions> 49. Best 10 bank reconciliation software, <https://www.nomentia.com/blog/best-10-bank-reconciliation-software> 50. The 20 Best Account Reconciliation Software Tools in 2025 - HighRadius, <https://www.highradius.com/resources/Blog/best-account-reconciliation-software/> 51. Bank Reconciliation Software: 5 Best Picks for Accuracy | Pilot Blog, <https://pilot.com/blog/best-bank-reconciliation-software> 52. The 10 best account reconciliation software in 2025 - Prophix, <https://www.prophix.com/blog/the-10-best-account-reconciliation-software/> 53. AI Change Management – Tips To Manage Every Level of Change | SS&C Blue Prism, <https://www.blueprism.com/resources/blog/ai-change-management/> 54. Unlocking AI Change Management in Financial Services - Bridgeforce, <https://bridgeforce.com/insights/unlock-ai-change-management-in-financial-services/> 55. The Importance of Change Management in AI Transformation - Consultport, <https://consultport.com/business-transformation/importance-of-change-management-in-ai-transf>

ormation/ 56. LLM Security: Risks, Best Practices, Solutions | Proofpoint US,  
<https://www.proofpoint.com/us/blog/dspm/llm-security-risks-best-practices-solutions> 57. LLM  
Security: Top 10 Risks and 7 Security Best Practices - Exabeam,  
[https://www.exabeam.com/explainers/ai-cyber-security/llm-security-top-10-risks-and-7-security-  
best-practices/](https://www.exabeam.com/explainers/ai-cyber-security/llm-security-top-10-risks-and-7-security-best-practices/) 58. LLM Security in 2025: Risks, Examples, and Best Practices,  
<https://www.oligo.security/academy/llm-security-in-2025-risks-examples-and-best-practices> 59.  
How to Use LLM with Private Data Best Practices for Data Security,  
[https://www.cognativ.com/blogs/post/how-to-use-llm-with-private-data-best-practices-for-data-  
se](https://www.cognativ.com/blogs/post/how-to-use-llm-with-private-data-best-practices-for-data-se) curity/263 60. Top 9 LLM Security Best Practices - Check Point Software Technologies,  
<https://www.checkpoint.com/cyber-hub/what-is-llm-security/llm-security-best-practices/>